UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,860	02/28/2002	Ronald P. Cocchi	PD-201161	1680

20991 7590 03/30/2006

THE DIRECTV GROUP INC
PATENT DOCKET ADMINISTRATION RE/R11/A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 03/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/085,860	COCCHI ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-15,17-25,27-40,42-45,47-55 and 57-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12,13,15,17-25,27,28,30-40,42,43,45,47-55,57 and 58* is/are rejected.

7)☒ Claim(s) *14,29,44 and 59* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/10/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the previous office actions, Applicant has amended claims 1, 15, 17, 30, 32, 45, and 47 and cancelled claims 11, 16, 26, 41, 46, and 56. Claims 1-10, 12-15, 17-25, 27-40, 42-45, 47-55, and 57-59 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 10 October 2005 has been fully considered.

Drawings

3. In view of Applicant's amendments to the specification, all previous objections to the drawings are withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 12, 13, 27, 28, 42, 43, 57, and 58 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Though the specification suggests the use of multiplexers with the hardware state machine, nowhere is it described the manner in which the multiplexers are actually used or configured.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 12, 13, 27, 28, 42, 43, 57, and 58 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: As discussed above, it is unclear how the multiplexers relate to the remainder of the invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 15, 17-19, 21-24, 30-34, 36-39, 45, 47-49, and 51-54 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6,035,038 to Campinos et al.

As per claims 15, 18, 30, 31, 33, 45, and 48, Campinos discloses a conditional access system wherein a security component implemented on a smartcard is used to decipher asynchronously transmitted entitlement messages for controlling access in an access control unit. The access control unit is not directly accessible to the system bus, and the smartcard ha no local bus (see figure 5 and column 5, lines 21-67).

As per claims 17, 32, and 47, this may be used on pay television (i.e. broadcast) systems (see column 1, lines 7-10).

As per claims 19, 34, and 49, the control words, which are used to descramble transmissions that have been encrypted by key K (see column 4, lines 3-16). The procedure for extracting the control words constitutes a key exchange protocol.

As per claim 21, 36, and 51, the enciphering key may be unique to a group (see column 6, lines 1-6).

As per claim 22, 37, and 52, since the access control register, where the keys must be stored, is not externally accessible, it constitutes a protected register.

As per claims 23, 24, 38, 39, 53, and 54, the authenticity of entitlement messages is verified using a hash algorithm (see column 5, lines 40-50) and the information is saved (see column 5, lines 51-58).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-10, 12, 15, 17-25, 27, 30-40, 42, 45, 47-55, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,157,719 to Wasilewski et al. in view of U.S. Patent No. 6,035,038 to Campinos et al.

As per claims 1, 2, 15, 30, 31, 45, Wasilewski discloses an access system for set-top boxes wherein configuration information may be transmitted to the set-top box as a one-time event (i.e. asynchronously). Since the set-top box's function is to determine whether an encrypted instance should be decrypted, it constitutes a security component that controls access to digital services. The received configuration information (the EMM) comprises decryption keys (control

words) to be implemented (see column 6, line 24 to column 7, line 24) in a hardware state machine (the DHCT) such as an ASIC (see column 15, lines 32-36 and figures 2B and 3). A control suite (the control center) sends transmissions via satellite, which inherently employs an uplink center for sending transmissions to the satellite. The stream is incorporated at a media server for distribution (see column 15, lines 7-24). The system comprises a smart card (see column 21, line 13).

The components of the DHCTSE, which contains the hardware state machine, are only accessible to the system bus or I/O via the DHCT interface. In Wasilewski's implementation, components of the DHCTSE communicate with one another via a local bus (see figure 12 and column 21, lines 15-27).

Campinos discloses a conditional access system wherein access control (the equivalent of the DHCTSE) is preformed on a user smartcard having no local bus and no direct outside access to the access control circuit (see figure 5 and column 5, line 28 to column 6, line 14) and suggests that this card makes it possible to verify that entitlements in the EMM are reserved for the user (see column 3, lines 48-57).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Wasilewski using the smartcard of Campinos for the DHCTSE, as this card makes it possible to verify that entitlements in the EMM are reserved for the user.

As per claims 17, 32, and 47, the configuration information may be sent over the broadcast channel, or another channel (see column 5, lines 6-11), such as the Internet (see column 7, lines 47-50).

As per claims 3-5, 18-20, 33-35, and 48-50, the configuration information is encrypted using a public key protocol such as RSA (see column 6, lines 60-66).

As per claims 6, 21, 36, and 51, the control words are encrypted using an algorithm having periodic key changes to the MSK (see column 6, lines 39-42 and 56-57). Wasilewski does not disclose the use of a group key.

Campinos discloses the use of a group key for encrypting entitlement messages, and suggests that this allows for a distribution arrangement wherein a key is not compromised outside of a group of users (see column 6, lines 1-6).

Therefore it would have obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Wasilewski using group keys, as this allows for a distribution arrangement wherein a key is not compromised outside of a group of users.

As per claims 7, 22, 37, and 52, the configuration information is decrypted at the DHCT, which is entirely protected in that it is only accessible through the encrypted interface, and placed in storage (registers) within the DHCT (see column 11, line 41 to column 12, line 21 and column 15, lines 63-64).

As per claims 8, 9, 23, 24, 38, 39, 53, and 54, the received EMM is only retained by the DHCT is the associated digest is confirmed as being correct (see column 11, lines 41-47).

As per claims 10, 25, 40, and 55, the entitlement agent may also directly provide encrypted instances to the entire service distribution organization, thereby making it a synchronous command (see column 12, lines 27-39). These are sent as Global Broadcast Messages (see column 13,lines 18-41).

As per claims 12, 27, 42, and 57, a demultiplexer (which is a type of multiplexer) is used at the beginning of the decryption process (see column 7, lines 8-16 and figure 2B).

8. Claims 13, 28, 43, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,157,719 to Wasilewski et al. in view of U.S. Patent No. 6,035,038 to Campinos et al. as applied to claims 1, 15, 30, and 45 above, and further in view of U.S. Patent No. 5,222,141 to Killian.

Wasilewski does not disclose the use of multiplexers after decryption.

Killian discloses the use of a multiplexer (MUX) at the end of an encryption/decryption process, and notes that it is used to select the input to be passed out of the scrambler stage (see column 2, lines 45-51). When performing a symmetric algorithm, such as DES, encryption and decryption circuits are interchangeable.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Wasilewski by using a multiplexor after the decryption stage, as disclosed by Killian, in order to select the input to be passed out of that stage.

Allowable Subject Matter

9. Claims 14, 29, 44, and 59 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter:

The closest prior art, cited above either discloses a smartcard in which the access control circuitry is directly connected to a smartcard's bus, or a smartcard having no bus. No art could be found in which hardware modules separate a conditional access module's bus from its access control circuitry.

Response to Arguments

11. Applicant's arguments, see Remarks, filed 11 January 2006, with respect to the rejections of claims 6, 21, 36, and 51 under 35 U.S.C. 112, second paragraph, have been fully considered and are persuasive In view of Applicant's explanation of the claim term. It is now understood that the term describes unique group keys. The rejections of claims 6, 21, 36, and 51 under 35 U.S.C. 112 have been withdrawn.

12. Regarding the rejections of claims 12, 13, 27, 28, 42, 43, 57, and 58 under 35 U.S.C. 112, first and second paragraphs, Applicant's arguments filed 11 January 2006 have been fully considered but they are not persuasive.

According to the Microsoft Computer Dictionary, 5th Edition, a multiplexer is used to either "attach many communications lines to a smaller number of communications ports or to attach a large number of communications ports to a smaller number of communications lines." Neither of these functionalities of a multiplexer results simply in the permuting of an input.

Applicant's specification simply states that the invention connects multiplexers using "custom logic" (see paragraph 70), without suggesting what that logic is. There exist many designs for permutors that are well-known in the art. For any digital logic design, there exists a large number of alternative designs, using different types of gates, that would produce the same set of outputs from the same respective inputs. It is therefore reasonable to conclude that it would be possible, given an arrangement of a number of multiplexers, to derive an output that is a rearrangement of an input. It would not, however, be clear to one of ordinary skill in the art (i.e. a journeyman digital logic designer) how to implement such a functionality without having to perform undue experimentation.

13. Applicant's arguments, see Remarks, filed 11 January 2006, with respect to the rejections of claims 1, 15, 30, and 45 under 35 U.S.C. 102 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn.

However, upon further consideration, a new ground(s) of rejection is made in view of Campinos.

Conclusion

14. Due to the new grounds of rejection, this action is non-final.

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques, can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

March 27, 2006